IGL502/752 – Techniques de vérification et de validation

Université de Sherbrooke

Examen final

Enseignant:	Michael Blondin
Date:	mercredi 16 décembre 2020
Durée:	3 heures

Directives:

- Répondez aux questions dans un **document électronique et/ou numérisé lisible**;
- Remettez vos solutions **préférablement au format PDF** et sur **Turnin**;
- L'examen se réalise en **3 heures**; vous avez une autre heure pour faire la remise;
- Donnez **une seule réponse** par sous-question;
- L'examen comporte **6 questions** sur **3 pages** valant un total de **50 points**;
- La correction se base notamment sur la **clarté**, l'**exactitude** et la **concision** de vos réponses, ainsi que sur la **justification** pour les questions qui en requièrent une;
- Les règles usuelles de plagiat s'appliquent; en particulier, **discuter de l'examen est du plagiat**.

Question 1: logique temporelle linéaire (LTL)

Soient *AP* $:= \{p, q\}$ et les formules LTL suivantes sur *AP*, où « $\oplus$ » dénote l'opération « OU exclusif »:

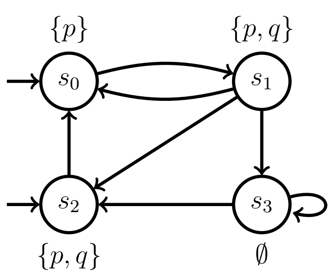
$$\varphi_1 := p \land \mathsf{FG}(p \oplus q) \qquad \varphi_2 := \neg p \;\mathsf{U}\; (\neg p \lor q) \qquad \varphi_3 := \mathsf{X}p \land \mathsf{G}(p \to \mathsf{F}q)$$

(a) Pour chaque formule φ_i, donnez un mot σ_i qui la satisfait et qui ne satisfait pas les deux autres, c.-à-d. 6 pts

$$\begin{array}{lll} \sigma_1 \models \varphi_1 & \sigma_1 \not\models \varphi_2 & \sigma_1 \not\models \varphi_3, \\ \sigma_2 \not\models \varphi_1 & \sigma_2 \models \varphi_2 & \sigma_2 \not\models \varphi_3, \\ \sigma_3 \not\models \varphi_1 & \sigma_3 \not\models \varphi_2 & \sigma_3 \models \varphi_3. \end{array}$$

(b) Donnez un mot σ qui satisfait à la fois φ_1, φ_2 *et* φ_3, c.-à-d. tel que $\sigma \models \varphi_1$, $\sigma \models \varphi_2$ et $\sigma \models \varphi_3$. 2 pts

(c) Pour chaque formule φ_i, dites si la structure de Kripke $\mathcal{T}$ ci-dessous satisfait φ_i. Justifiez. 3 pts



Question 2: langages ω-réguliers

(a) Donnez une expression ω-régulière et un automate de Büchi pour ce langage: 3 pts

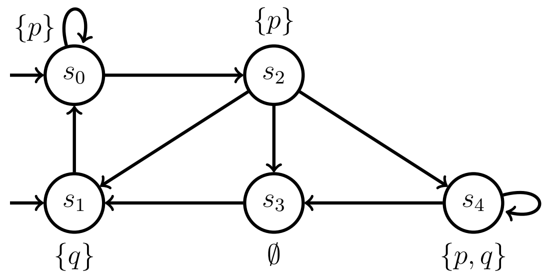
$$L := \{\sigma \in \{a, b, c\}^\omega : \underbrace{(\exists i \in \mathbb{N} : \sigma(i) = a) \land [\forall i \in \mathbb{N} : (\sigma(i) = a) \to (\exists j > i : \sigma(j) = b)]}_{\text{« } \sigma \text{ contient au moins un } a\text{, et chaque } a \text{ est éventuellement suivi d'un } b \text{ »}}\}$$

(b) Donnez un automate de Büchi $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{B}) = [\![\neg\mathsf{X}p \lor \mathsf{G}(p \;\mathsf{U}\; q)]\!]$ sur alphabet $\Sigma := \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$. 3 pts

Question 3: logique temporelle arborescente (CTL) et vérification symbolique

Rappel: l'abbréviation « BDD » réfère à « diagramme de décision binaire (ordonné et réduit) ».

Supposons que chaque état de la structure de Kripke $\mathcal{T}$ ci-dessous soit codé par la représentation binaire de son indice; autrement dit: $s_0 = 000$, $s_1 = 001$, $s_2 = 010$, $s_3 = 011$ et $s_4 = 100$ (les autres chaînes sont invalides).



(a) Pour chaque formule Φ ci-dessous, donnez l'ensemble $[\![\Phi]\!]$ des états de $\mathcal{T}$ qui satisfont Φ, et dites si $\mathcal{T} \models \Phi$. 6 pts

(i) $\exists(p \mathbin{\mathsf{U}} q)$ (ii) $\forall(p \mathbin{\mathsf{U}} q) \land \exists\mathsf{G}(p \lor q)$ (iii) $\forall\mathsf{X}\,\exists(p \mathbin{\mathsf{U}} q)$

(b) Donnez un BDD qui représente les états initiaux I. *Remarque: Il n'est pas obligatoire d'appliquer un algorithme.* 2 pts

(c) Donnez un BDD qui représente l'ensemble $[\![p]\!]$. *Remarque: Il n'est pas obligatoire d'appliquer un algorithme.* 2 pts

(d) Expliquez comment vérifier algorithmiquement si $\mathcal{T} \models \neg p$ à partir des BDDs construits en (b) et (c). 2 pts

Question 4: systèmes à pile

Considérons le programme suivant constitué de deux fonctions et d'une variable booléenne globale `x`, dont le point d'entrée est `main`, et où « `?` » dénote un choix non déterministe:

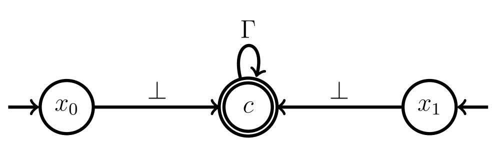
```
      bool x ∈ {faux, vrai}

      main():                    foo(bool y):
m0:     si ?:              f0:     x = x ∨ y
          x = vrai
m1:       foo(¬x)
        sinon:
          main()
m2:     assert(x)
```

(a) Pourquoi ne peut-on pas modéliser ce programme à l'aide d'une structure de Kripke finie? 1 pt

(b) Modélisez le programme avec un système à pile $\mathcal{P}$. 3 pts

(c) Construisez partiellement un $\mathcal{P}$-automate $\mathcal{B}$ qui accepte $\text{Pre}^*(\mathit{Conf}(\mathcal{A}))$, où $\mathcal{A}$ est ce $\mathcal{P}$-automate: 3 pts

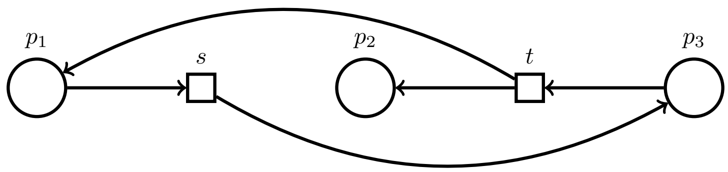


Plus précisément, ajoutez *trois nouvelles transitions* à $\mathcal{A}$ en exécutant l'algorithme de saturation vu en classe. Au moins deux de ces transitions doivent être obtenues *sans* utiliser une transition de $\mathcal{P}$ étiquetée par une règle de la forme « *lettre* $\to \varepsilon$ ».

Rappel: Γ *est l'alphabet de* $\mathcal{P}$.

Question 5: réseaux de Petri

Soit le réseau de Petri $\mathcal{N} = (P, T, F)$ suivant:



(a) Complétez ce graphe de couverture de $\mathcal{N}$ qui débute au marquage $\boldsymbol{m} \coloneqq (1, 1, 1)$: 3 pts

$$\begin{tikzcd} & (1,1,1) \arrow[dl, "s"'] \arrow[dr, "t"] & \\ (0,1,2) & & (2,2,0) \end{tikzcd}$$

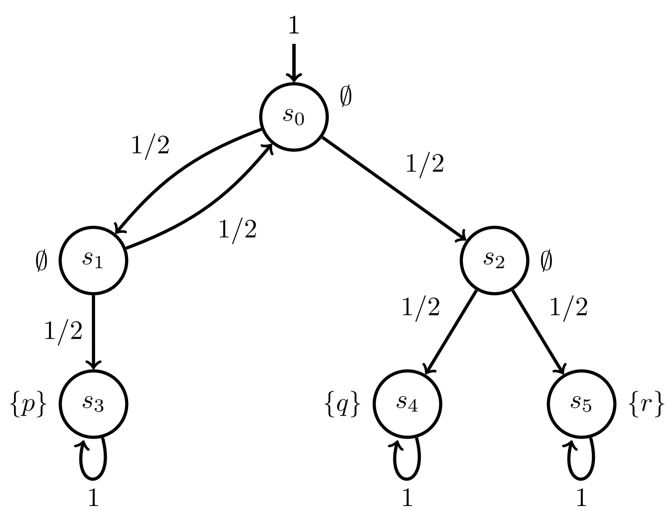
(b) Dites lesquels de ces marquages sont couvrables à partir de $\boldsymbol{m}$. Justifiez brièvement. 1,5 pts

$$\boldsymbol{m}_0 \coloneqq (2, 1, 1), \qquad \boldsymbol{m}_1 \coloneqq (1, 2, 1), \qquad \boldsymbol{m}_2 \coloneqq (1, 1, 2)$$

(c) Rappelons que chaque itération de l'algorithme arrière ajoute $|B| \cdot |T|$ marquages à la base actuelle B, puis la minimise. La taille de la base B augmente-t-elle systématiquement à chaque itération, ou est-ce possible que sa taille augmente pendant quelques itérations, puis diminue à un certain point? Justifiez. 2,5 pts

Question 6: chaînes de Markov

La chaîne de Markov $\mathcal{M}$ ci-dessous cherche à simuler un dé à trois faces, c.-à-d. qu'on aimerait qu'elle satisfasse la propriété PCTL $\varphi \coloneqq \mathcal{P}_{=1/3}(\mathsf{F}\, p) \land \mathcal{P}_{=1/3}(\mathsf{F}\, q) \land \mathcal{P}_{=1/3}(\mathsf{F}\, r)$.



(a) Dites si on a bien $\mathbb{P}(s_0 \models \mathsf{FG}\, A) = 1$, où $A \coloneqq \{s_3, s_4, s_5\}$. Justifiez. 2 pts

(b) Quelle est la valeur de $\mathbb{P}(s_0 \models \mathsf{F}\, s_2)$? Justifiez. 3 pts

(c) Est-ce que $\mathcal{M}$ satisfait la propriété φ? Autrement dit, est-ce que $s_0 \models \varphi$? Justifiez. 2 pts